⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−43734

⑤1Int.Cl.⁵	識別記号	庁内整理番号	⑬公開 平成4年(1992)2月13日
H 04 L 9/32			
G 06 F 15/00	330 B	7218−5L	
H 04 L 12/22			
		7117−5K H 04 L 9/00	A
		7830−5K 11/26	

審査請求 未請求 請求項の数 1 (全6頁)

⑤4発明の名称　対話型個人認証装置

⑳特　願 平2−151840
㉒出　願 平2(1990)6月11日

⑦2発明者　宮内　直人　神奈川県鎌倉市大船5丁目1番1号　三菱電機株式会社情報電子研究所内
⑦1出願人　三菱電機株式会社　東京都千代田区丸の内2丁目2番3号
⑦4代理人　弁理士　宮園　純一

明　細　書

1. 発明の名称

対話型個人認証装置

2. 特許請求の範囲

ネットワーク上のコンピュータの利用者を識別する対話型個人認証装置において、利用者の名前などを示す識別子とそのパスワードを対にして予め記憶する第1記憶部と、利用者から入力した識別子を上記第1記憶部に記憶された識別子と比較することにより、識別する名前識別部と、上記第1記憶部に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する合成パスワード発生部と、上記第1記憶部に記憶された利用者のパスワードと上記合成パスワードとの差分である合成認証情報を記憶する第2記憶部と、利用者から送られてきた合成認証情報と上記第2記憶部に記憶された合成認証情報とを比較し利用者の認証を行う認証識別部とを備えたことを特徴とする対話型個人認証装置。

3. 発明の詳細な説明

(産業上の利用分野)

この発明はネットワーク上のコンピュータへアクセスする場合の利用者の認証を行う対話型個人認証装置に関するものである。

(従来の技術)

従来、この種の対話型個人認証方法としては例えば、

カール.H.マイアー、スティーブン.M.マティス共著

「暗号」自然社(昭61-2-10)p.358-p.394

D.W.Davies,W.L.Price共著

「ネットワークセキュリティー」日経マグロウヒル社(昭60-12-5)p.111-p.132

小林、山本

「5U-7 ソフトウェアの権利保護のためのアクセス制御方式」「第33回全国大会講演論文集」情報処理学会(昭61-10-1)p.1097-p.1098

CCITT

「Recommendation X.509 The Directory-Authentication Framework」(1988-12)p.12-p.14

に示されたようなものがあった。

第５図は従来の対話型個人認証装置の構成を示すブロックである。第５図において、５１は利用者の認証を行う認証サーバである。この認証サーバ５１は、認証クライアント５６から利用者の識別子とそのパスワードを入力したりするサーバ側入出力部５２と、利用者の識別子とそのパスワードを対にして記憶する第１記憶部５５と、サーバ側入出力部５２によって入力された利用者の識別子を第１記憶部５５に記憶されている利用者の識別子と比較し利用者の名前の妥当性を評価する名前識別部５３と、サーバ側入出力部５２によって入力された利用者のパスワードを第１記憶部５５に記憶されている利用者のパスワードと比較し認証情報の妥当性を評価する認証識別部５４とを備えている。認証クライアント５６は、認証サーバ５１に対して認証操作を行うクライアントである。クライアント側入出力部５７は、利用者が識別子とパスワードを入力し、これらを認証サーバ５１へ送信するものである。伝送路５８は利用者の識別子とパスワードを伝送するためのものである。

次にこの従来例の動作を第６図のフローチャートを参照して説明する。まず、ステップ６１でサーバ側入出力部５２から利用者の識別子Ｎ１とパスワードＰ１を入力する。次にステップ６２で名前識別部５３がステップ６１で入力された識別子Ｎと第１記憶部５５に登録〔記憶されている識別子Ｎ０とを比較し両者が同一ならばステップ６３を実行し、異なる場合は認証不正となり処理を終了する。ステップ６３では入力した識別子Ｎ０に対応するパスワードＰ１を第１記憶部５５から取得する。次にステップ６４で認証識別部５４が入出力部５２から入力したパスワードＰ０を第１記憶部５５に登録されているパスワードＰ１と比較し両者が同一ならば認証が正常に終了する。両者が異なる場合は認証不正となり処理を終了する。

このように、従来の対話型個人認証装置は、利用者を識別するために、サーバ側入出力部５２から識別子とパスワードを入力し、第１記憶部５５に記憶されている識別子とパスワードを比較することによって、利用者の認証を行うように構成されている。

〔発明が解決しようとする課題〕

以上のような従来の対話型個人認証装置は、利用者の識別子とパスワードによって、暗号技術を使った認証よりも簡易に認証を行えるが、ネットワークの伝送路上に利用者の識別子とパスワードが流れるため、それらが盗聴されるおそれがあり、また、盗聴防止のためには暗号化処理を行う方法もあるが、従来の方法は処理が複雑であるという問題点があった。

この発明は上記のような問題点を解決するためになされたもので、高度な暗号化技術を使わなくても、登録されているパスワードが伝送路上から盗聴されることを防ぐことができる対話型個人認証装置を提供することを目的とする。

〔課題を解決するための手段〕

この発明に係る対話型個人認証装置は、利用者の名前などを示す識別子とそのパスワードを対にして予め記憶する第１記憶部５と、利用者から入力した識別子を第１記憶部５に記憶された識別子と比較することにより識別する名前識別部３と、第１記憶部５に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する合成パスワード発生部７と、第１記憶部５に記憶された利用者のパスワードと上記合成パスワードとの差分である合成認証情報を記憶する第２記憶部６と、利用者から送られてきた合成認証情報と第２記憶部６に記憶された合成認証情報とを比較し利用者の認証を行う認証識別部４とを備えたものである。

〔作用〕

第１記憶部５は利用者の識別子とそのパスワードを対にして予め記憶する。名前識別部３は、利用者から入力した識別子を、第１記憶部５に記憶された識別子と比較することにより識別する。合成パスワード発生部７は第１記憶部５に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する。第２記憶部６は利用者のパスワードと合成パスワードとの差分である合成認

証情報を記憶する。認証識別部４は利用者から送られてきた合成認証情報と第２記憶部６に記憶されている合成認証情報とを比較し利用者の認証を行う。

（実施例）

第１図はこの発明の一実施例に係る対話型個人認証装置の構成を示すブロック図である。第１図において、１は利用者の認証を行う認証サーバである。認証サーバ１は認証クライアント８から利用者の識別子と合成認証情報を入力し認証クライアント８に合成パスワードを出力するサーバ側入出力部２と、このサーバ側入出力部２から入力した利用者の名前などを示す識別子を第１記憶部５に記憶された識別子と比較することにより識別する名前識別部３と、サーバ側入出力部２より入力した利用者からの合成認証情報と第２記憶部６に記憶された合成認証情報とを比較し利用者の認証を行う認証識別部４と、利用者の識別子とそのパスワードを対にして予め記憶する第１記憶部５と、第１記憶部５に記憶された利用者のパスワードと合成パスワードとの差分である合成認証情報を記憶する第２記憶部６と、第１記憶部５に記憶された利用者のパスワードをランダムに変更して合成パスワードを発生する合成パスワードを発生部７とを備えている。認証クライアント８は、認証サーバ１に対して認証操作を行うクライアントであり、利用者の識別子と合成認証情報を入力してこれらを認証サーバ１に送信し、また、認証サーバ１から入力した合成パスワードを利用者に出力するクライアント側入出力部９を備えている。伝送路１０は、認証サーバ１と認証クライアント８間で、利用者の識別子、合成パスワード、合成認証情報などを伝送するものである。

第２図は認証サーバ１が利用者の認証を行う際の手続きを示すフローチャートで、第３図は認証クライアント８が利用者の認証手続きを行う際のフローチャートである。

次にこの実施例の動作について第１図～第３図を参照して説明する。

まず、第３図において、ステップ２１でクライアント側入出力部９が、利用者から識別子Ｎ１を入力する。次に、ステップ２２でクライアント側入出力部９が、認証サーバ１に利用者の識別子Ｎ１を出力する。

次に、第２図において、ステップ１１で、サーバ側入出力部１が認証クライアント８から利用者の識別子Ｎ１を入力する。次に、ステップ１２で名前識別部３はステップ１１で入力した利用者の識別子Ｎ１を第１記憶部５に登録されている利用者の識別子Ｎ０と比較し、利用者の識別子Ｎ１の正誤を判別する。利用者の識別子Ｎ１が正しければ、ステップ１３を実行する。次にステップ１３で、ステップ１２で入力した識別子Ｎ１と対をなすパスワードＰ０を第１記憶部５から検索する。次にステップ１４で、合成パスワード発生部７が、パスワードＰ０を基に合成パスワードＰ１を生成する。次に、ステップ１５で、ステップ１４で得られた合成パスワードＰ１とステップ１３で得られたパスワードＰ０の差分の文字例を合成認証情報Ｄ０として、第２記憶部６に記憶する。次に、ステップ１６で、ステップ１５で得られた合成パスワードＰ１をサーバ側入出力部２から伝送路１０を通して、認証クライアント８に出力する。

次に第３図において、ステップ２３で、認証クライアント８のクライアント側入出力部９において、認証サーバ１から合成パスワードＰ１を入力する。次に、ステップ２４でクライアント側入出力部９が利用者に合成パスワードＰ１を出力する。次に、ステップ２５で、クライアント側入力部９が利用者から合成認証情報Ｄ１を入力する。この時、合成認証情報Ｄ１は、利用者が記憶しているパスワードと合成パスワードの差分である。次に、ステップ２６で、認証クライアント８のクライアント側入出力部９において、ステップ２５で得られた合成認証情報Ｄ１を伝送路１０を通して認証サーバ１に出力する。

次に、第２図において、ステップ１７で、認証サーバ１のサーバ側入出力部２において、認証クライアント８から合成認証情報Ｄ１を入力する。ステップ１８で、認証識別部４がステップ１７で

入力した合成認証情報Ｄ１とステップ１５で記憶した合成認証情報Ｄ０を比較する。比較結果が正しければ、利用者の認証を完了する。

このようにして、伝送路１０に利用者のパスワードを流すことなく、また複雑な暗号手法を使わずに、ネットワークにおける盗聴を回避できる。

第４図は他の実施例の構成を示すブロック図であり、第４図において第１図に示す構成要素に対応するものには同一の符号を付し、その説明を省略する。第４図において、４１は認証クライアント８に備えられるパスワード変換部である。第１図の実施例では、認証クライアント８のクライアント側入出力部９が利用者から合成認証情報Ｄ１を入力して認証を行うものについて説明したが、第４図の実施例の場合、利用者は従来通りのパスワードＰ２を認証クライアント８に入力し、パスワード変換部４１がそのパスワードＰ２と認証サーバ１から送られてくる合成パスワードＰ１とを比較して、合成認証情報Ｄ１を生成する。このようにすれば、第１の実施例と同様の効果があるのに加え、利用者インタフェースに従来の認証手段と同じものが使用できるため、利用者から新しい認証手段を隠蔽できるという効果がある。

以上説明したように上記各実施例は、利用者の識別子をサーバ側入出力部２から入力し、この入力した識別子と第１記憶部５に記憶されている識別子とを名前識別部３で比較し、合成パスワード発生部７で識別子と対になっているパスワードをランダムに合成し、この合成したパスワードと第１記憶部５に記憶されているパスワードとの差分を合成認証情報として第２記憶部６に記憶し、サーバ側入出力部２においてその合成パスワードを認証クライアント８に出力し、また、認証クライアント８を通じて利用者から合成認証情報を入力し、認証識別部４において、入力した合成認証情報と第２記憶部６に記憶されている合成認証情報とを比較し、その結果により利用者の認証を行うように構成されている。

上記各実施例によれば、認証のために認証サーバ１と認証クライアント８間で２往復のアクセスを行い、伝送路１０上にパスワードを送信しないため、伝送路１０におけるパスワードの盗聴を防止することができる。

〔発明の効果〕

以上のように本発明によれば、利用者のパスワードをランダムに変更して合成パスワードを生成し、利用者のパスワードと合成パスワードとの差分である合成認証情報を記憶させ、この記憶された合成認証情報と利用者から送られてきた合成認証情報とを比較することにより、利用者の認証を行うように構成したので、高度な暗号化技術を使わなくても、登録されているパスワードが伝送路上から盗聴されることが防止でき、これにより、従来のパスワードによる認証よりも安全性が高まる上、利用者はパスワードの他に認証情報を覚える必要がなく、従来の暗号化技術よりも容易にパスワードを隠蔽できるという効果が得られる。

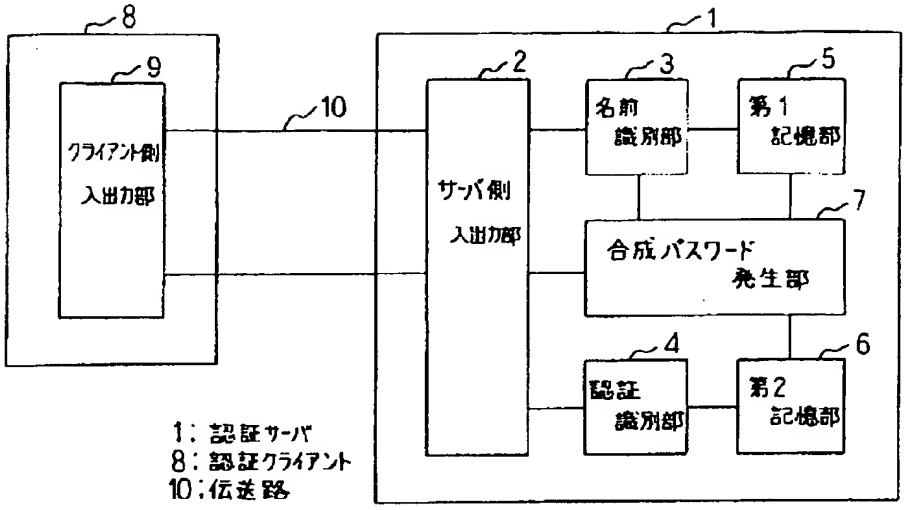
4. 図面の簡単な説明

第１図はこの発明の一実施例に係る対話型個人認証装置の構成を示すブロック図、第２図は第１図中の認証サーバが利用者の認証を行う際の手続きを示すフローチャート、第３図は第１図中の認証クライアントが利用者の認証手続きを行う際のフローチャート、第４図は他の実施例に係る対話型個人認証装置の構成を示すブロック図、第５図は従来の対話型個人認証装置の構成を示すブロック図、第６図はこの従来装置の認証動作を示すフローチャートである。

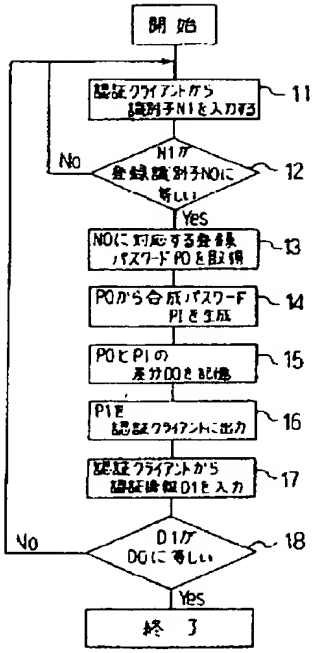
３・・・名前識別部、４・・・認証識別部、５・・・第１記憶部、６・・・第２記憶部、７・・・合成パスワード発生部。

代理人　弁理士　宮　園　純　一

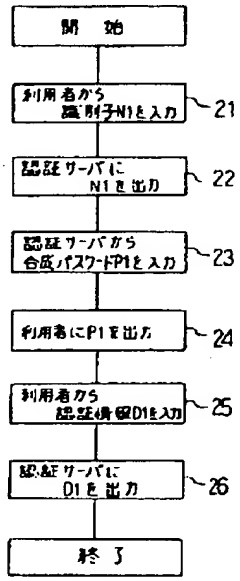
第 1 図



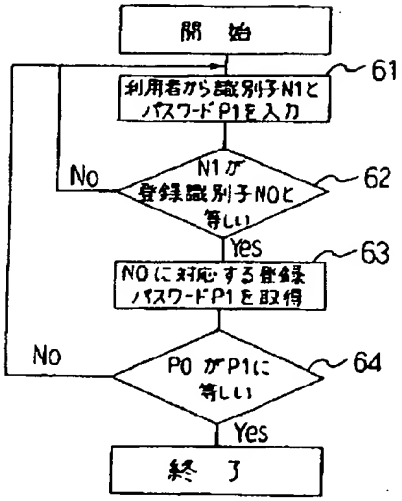
第 2 図



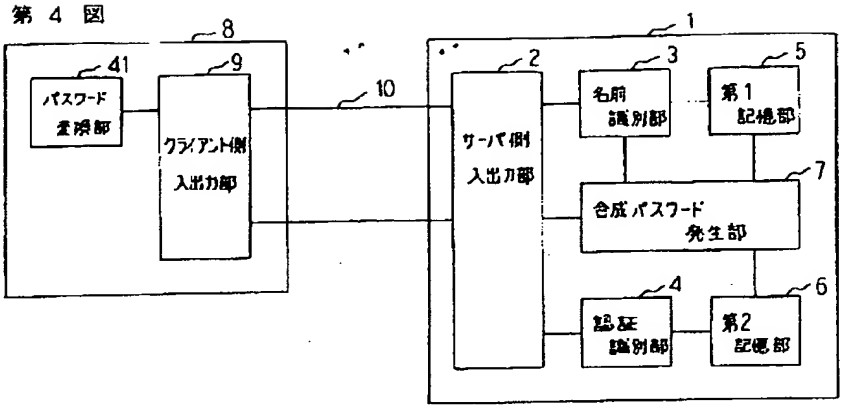
第 3 図



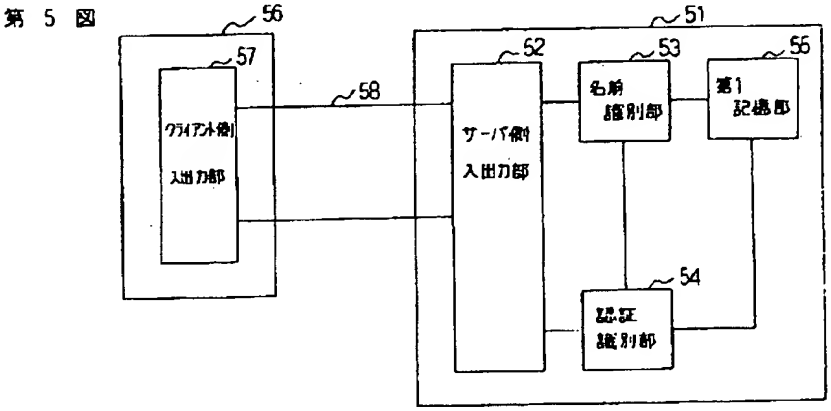
第 6 図



第４図



第５図



手　続　補　正　書　（自発）

平成　２年　７月27日

特許庁長官殿

１．事件の表示　　特願平２－１５１８４０号

２．発明の名称

対　話　型　個　人　認　証　装　置

３．補正をする者

事件との関係　特許出願人
住　所　東京都千代田区丸の内二丁目２番３号
名　称　(601)三菱電機株式会社
代表者　志　岐　守　哉

４．代　理　人

住　所　東京都千代田区飯田橋二丁目９番４－４０５
宮園国際特許事務所
氏　名　(8029)弁理士　宮　園　純　一
(連絡先03(234)5650)

５．補正の対象

明細書の発明の詳細な説明の欄。

６．補正の内容

(1)明細書の第４頁第７行目「登録（記憶されている」とあるのを「登録（記憶）されている」と補正する。

以　上

方式審査　閲川　特許 2.9.29 出願 山本